NAK1-BP89

PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	Examiner:
Osamu Shibata, et al.	Group Art Unit: 2131
Serial No.: 09/936,157	
Filed: September 6, 2001	
For: AUTHENTICATION COMMUNICATION APPARATUS AND AUTHENTICATION COMMUNICATION SYSTEM	March 5, 2002 Irvine, California 92614

PETITION TO MAKE SPECIAL

Assistant Commissioner for Patents
Washington, D.C. 20231

Dear Sir:

In accordance with MPEP Section 708.02(viii), Applicant hereby requests that the above-identified application be made special and the fee in accordance with 37 C.F.R. Section 1.17(i) is submitted herewith.

It is believed that all of the claims are directed to a single invention. If, however, it is determined that the claims are not directed to a single invention, Applicant hereby agrees to elect, without traverse, as a prerequisite to the granting of a special status.

An international search has been made in the Japanese Patent Office in International Application No. IA PCT/JP01/00159. A copy of the International Search Report, together

with copies of the references cited, are already of record in this application. The present claims and subject matter was examined by the Japanese Patent Office.

The International Search Report cited the Japanese Laid Open Patent Application No. H10-51439 which corresponds to U.S. Patent No. 6,058,476 (copy attached). This reference discloses an encryption apparatus wherein a random number is transferred between a first device A and a second device B in a challenge-response authentication format. The random number is used as a key for a session (data reading or writing session) and encrypted communication of confidential data can then be carried out by exploiting the increased time-variableness of the key.

The present invention sets forth an authentication communication system with a first authentication phase wherein the access device authenticates whether a storage medium is authorized in a challenge-response authentication protocol by transmitting scrambled access information generated by scrambling access information which shows the area to the storage medium. A second authentication phase occurs in which the storage medium authenticates whether the access device is authorized, and a transfer phase occurs after the authentication wherein the storage medium extracts the access information from the scrambled access information to enable the access device to either read or write digital information from or into the area shown by the access information.

The present application embeds information for accessing the confidential data storage area in a random number which is transferred for the challenge-response authentication. Therefore, even after the authorized devices succeed in mutual authentication, an unauthorized device can not intrude and impersonate one of the

authorized devices, since the unauthorized device can not designate the confidential data storage area, and therefore, can not access the confidential data.

The '476 patent does not take into consideration the security of the access information, since it does not link the mutual authentication to authenticate the devices in communication with the conveyance of access information to access the confidential data as defined by access information, such as address and size of the storage area.

The Japanese Laid Open Patent Application No. H11-306673 was also cited as a relevant reference for a combination with a secondary reference. This reference discloses a method of safely storing confidential information on a storage device (DVD, ROM, MO, HDD, etc.) in a PC. The storage device can be divided into a general area and a confidential data storage area that is difficult to access to enhance security against unauthorized access. As noted above, the present application embeds information, such as address and size of the storage area, in a random number which is transferred for a challenge response authentication. The Japanese Laid Open Patent Application '673 does not suggest nor provide a construction that links the mutual authentication between devices to authenticate the devices in communication by the conveyance of access information to access the confidential data.

The Japanese Laid Open Patent Application No. H08-056387 discloses a method of varying an I.D. which can be sent/received to reset a key in a keyless security system of a car. As mentioned above, the present application relates to a specific construction of embedding access information that can be used in a mutual authentication procedure. The '387 Laid Open reference relies merely on authentication procedure and therefore can not replicate nor suggest the effects of the present application. Even if this cited reference was

attempted to be combined with the above documents, the construction of embedding the access information in a mutual authentication procedure would not be taught.

Finally, the Japanese Laid Open Patent Application No. H07-311674 teaches a pseudo-random number generation device that generates a new random number using both a time-varying counter value and a random number generated by a random number function circuit, so that an unbiased random number is generated even when the random number function circuit is initiated. As noted, the present invention scrambles access information during a first authentication phase for a mutual authentication procedure. The '674 Laid Open reference relates only to a random number generation device, and therefore, can not deliver the effects and advantages of the present claims. Again, since this reference would lack the essential teachings of the present invention. Even if it is combined with the other references cited above, it would not be capable of anticipating or rendering obvious the present claims.

The remaining reference was simply cited as a document in the same patent family, and is not as relevant as the references cited above.

In summary, the present invention is defined in the presently pending claims and provides an authentication communication device with a storage medium having an area for storing digital information therein, and an access unit for reading digital information from that area and writing digital information into the area. The access unit authenticates the storage medium according to a challenge response authentication protocol using a disturbed access information produced by disturbing access information indicative of the area. The access unit is authenticated by the storage medium. When authenticated, the access unit can

read out or write into the storage medium corresponding to the access information separated from the disturbed access information.

As set forth above, it is believed that the references cited in the PCT Search Report fail to teach the advantageous features set forth in the presently pending claims.

It is believed that all the requirements to have the present application made special have been complied with. If there are any questions or additional requirements, the undersigned attorney would appreciate a telephone conference.

I hereby certify that this correspondence is being deposited with the United States Postal Service as First Class Mail in an envelope addressed to the Assistant Commissioner for Patents, Washington, D.C. 20231 on March 6, 2002.

By: Marc Fregoso

Marc Fregoso

Signature

Date: March 6, 2002

Respectfully submitted,

PRICE AND GESS

Joseph W. Price
Registration No. 25,124
2100 S.E. Main St., Suite 250
Irvine, California 92614
Telephone: 949/261-8433